NATIONAL ACADEMY OF PUBLIC ADMINISTRATION
1600 K Street, N.W., Suite 400
Washington, D.C. 20006
TEL: (202) 347-3190 FAX: (202) 223-0823
INTERNET: www.napawash.org

Written Testimony of Dr. Alan R. Shark

Fellow, National Academy of Public Administration

and

President and CEO, Public Technology Institute

Before the Committee on Ways and Means

Subcommittee on Social Security

U. S. House of Representatives

February 26, 2014

Chairman Johnson, Ranking Member Becerra, and Members of the Subcommittee:

Thank you for the invitation to testify today to discuss high-impact, valuable, and feasible recommendations that can assist the Social Security Administration (SSA) in preventing and detecting conspiracy fraud in the Social Security Disability Insurance program (SSDI). It is an honor to contribute to this important discussion.

I am a Fellow and Chair of the Technology Leadership Standing Panel at the National Academy of Public Administration (the Academy). Established in 1967 and chartered by Congress, the Academy is an independent, non-profit, and non-partisan organization dedicated to helping leaders address today's most critical and complex challenges. The Academy has a strong organizational assessment capacity; a thorough grasp of cutting-edge needs and solutions across the federal government; and unmatched independence, credibility, and expertise. Our organization consists of nearly 800 Fellows—including former cabinet officers, Members of Congress, governors, mayors, and state legislators, as well as distinguished scholars, business executives, and public administrators. The Academy has a proven record of improving the quality, performance, and accountability of government at all levels.

I am also the Executive Director and CEO of the Public Technology Institute and Associate Professor of Practice at Rutgers University School of Public Affairs & Administration.

As an Academy Fellow, I served as Panel Chair for the Academy's work with the Recovery Accountability and Transparency Board (RATB) on the "National Dialogue on Innovative Tools to Prevent and Detect Fraud, Waste and Abuse." Facing similar challenges to SSA, RATB sought to identify new tools and strategies by which it might prevent and detect fraud, waste, and abuse. The Academy is currently working with SSA on a congressional mandate that includes developing a high-level plan to assist the agency in addressing service delivery challenges in the coming ten to fifteen years. In working on the long-term strategic plan for SSA, the Academy has identified several imperatives that describe SSA's approach to rendering its services, including maintaining the public trust and enhancing program integrity. That said, it is

important to note that this current study does not address the issue of deterring disability insurance fraud.

My comments today represent my own views and also derive in part from the recommendations issued by an independent Panel of the Academy to the Recovery Board following the results of the national dialogue.

Summary

The SSA OIG identified an urgent need for SSA to adopt more effective methods to detect fraud earlier in the disability claims process, particularly with regard to "facilitator fraud," like that which occurred in Puerto Rico and New York. These cases highlighted the deleterious effects of unchecked conspiracy fraud and the importance of leveraging technology to strengthen SSA's capacity to intercept suspicious activity at its inception. This task is complicated by the disability program's complex eligibility rules, multiple layers of review, and multiple handoffs from one person to another at the state and federal level. In order to optimize its capacity for preventing payments on fraudulent disability claims, SSA must focus its efforts on implementing the newest analytic tools for fraud detection used by the private sector, while also developing a culture of fraud prevention and openness to new technology across SSA. SSA's Office of Disability Adjudication Review (ODAR) has already paved the way for these changes through its effort to more consistently and accurately process benefits appeals using case analysis tools and analytical methods. Furthermore, SSA should incorporate warnings at the beginning of the application process clearly stating SSA's advanced capacity for detecting fraud and the consequences of defrauding the federal government. By implementing agency-wide changes to its IT infrastructure and work culture, SSA can restore confidence in the disability program and ensure that taxpayer dollars are spent wisely and efficiently.

The recommendations presented today are intended to support the current anti-fraud efforts SSA is in the process of planning and implementing.

SSA must develop an IT system that incorporates textual analysis tools and predictive analytics technology to maximize its ability to detect disability insurance fraud.

SSA's "pay and chase" methods have yielded success in detecting improper disability payments, however, it is critical that SSA increase its capacity to prevent fraud rather than respond to it. To do this, SSA must move beyond its reliance on the integrity of the participants in the complex benefits application process. This includes SSA's own employees, State and Commonwealth Disability Determination Services (DDS) employees, claimants, and third party claimant representatives -- including attorneys, doctors, and interpreters, who are collectively relied upon to serve as primary sources of fraud detection. While State DDS and SSA employees are credited with bringing alleged fraudulent activities in Puerto Rico and New York to the attention of the OIG, SSA must also implement technology driven detection methods capable of flagging fraudulent activity more consistently, systematically and accurately. Early detection of suspicious activity is imperative to prevention.

The unstructured data stored by SSA regarding disability claims processing holds critical information that data analytical tools can utilize to find patterns indicative of fraudulent activity. Automated textual analysis and mining of unstructured data, also known as Natural Language Processing (NLP) or Statistical NLP tools, have the potential to prevent and detect fraud in addition to streamlining bureaucratic processes. Tools are available that automate the scanning of lengthy government documents, which are replete with this unstructured, semi-structured, as well as more standard structured data, into rows and columns. The tools can convert free-form text into relational tables and fuse this data with structured data. In order to maximize the benefit of these types of data mining tools, SSA must take steps to ensure digitization of disability benefit applications and associated records.

Predictive analytics technology is another tool that involves pattern recognition among data sources. For example, when State DDS offices collect medical records and other documentation used to review disability claims, they are developing a database of critical data points that can be mined to create visual data patterns, such as "heat mapping." For example, a particular office

may suddenly experience an increased volume in claimants with similar disabilities, whose medical records are being provided by the same physician, or who are being represented by the same attorney. Similar key identifying factors were present in the recent alleged organized fraud in New York with several beneficiaries claiming injuries related to the 9/11 attacks and using common facilitators throughout the process. Heat mapping would have presented a visual influx of these commonalities which may have led to a more expedient awareness of potential fraudulent activity.

The Department of Health and Human Services (HHS) has successfully implemented predictive analytics technology to deter Medicare and Medicaid fraud by running analytics on claims nationwide. Facing similar challenges in combatting fraud, waste, and abuse in the administration of benefits, HHS and the Centers for Medicare and Medicaid Services (CMS) launched a national effort in 2010 to prevent fraud. Since enactment of the Affordable Care Act, CMS has also implemented new anti-fraud tools provided by Congress in addition to shifting to an innovative approach that identifies fraud before payments are made instead of a "pay and chase" approach. CMS's Center for Program Integrity (CMP) uses state-of-the-art predictive analytics technology, the Fraud Prevention System (FPS), to identify and prevent fraud, waste and abuse in the Medicare fee-for-service (FFS) program. The FPS is able to run sophisticated analytics nationwide against all Medicare FFS claims prior to payment to identify aberrant and suspicious billing patterns, enabling CMS to work toward stopping payments as soon as problems are detected. The FPS reported that CMS stopped, prevented, or identified an estimated $115.4 million in payments in its first year.

Since June 30, 2011, CMS has been screening all Medicare FFS claims nationwide and prepayment with the predictive analytics technology of the new FPS. Through procedures under the Federal Acquisition Regulation, CMS partnered with industry-leading private-sector contractor teams to adapt existing telecommunications and banking industry anti-fraud technology to the unique requirements of combatting Medicare fraud. It is also worth noting that CMS implemented a governance process to provide oversight, management, and control in the selection of new models, model enhancements, and system changes to improve the FPS. This

process enables CMS to respond to vulnerabilities identified by the OIG, GAO and other stakeholders with adaptive fraud-detection models.

By combining data analysis tools and predictive analytics technology with its current fraud detection training of field officers and DDS employees, SSA could significantly increase its success in the early detection of potential and actual fraud.

SSA could better leverage data sources, including state and local governmental data and proprietary business data to improve data validation in predicting potential fraud and abuse.

Fostering a culture of collaboration and information sharing provides another level of protection against fraud. OIG and SSA jointly established the Cooperative Disability Investigation (CDI) Program to pool resources, including databases, from State DDS offices and State and local law enforcement agencies. Web-scraping tools are available to pull quality state and local data, enabling SSA and CDI to better leverage these resources. The New York conspiracy fraud case is a perfect illustration of the importance of leveraging state and local data. The NYPD licensing division maintains records on individuals holding gun permits and applicants must certify that they have no mental impairments. Many of the beneficiaries suspected of defrauding the disability insurance program were retired police officers claiming mental impairment. Acting on the knowledge that retired police officers often apply for gun permits to procure employment, the New York CDI unit was able to cross check gun permit applicants with the beneficiaries in question and discovered they had in fact applied for permits. Connecting these seemingly unrelated data elements provided the evidence needed to uncover an elaborate scheme to defraud SSA. Applying advanced technology to pooled data sources will enhance CDIs efforts to fulfill its primary mission of obtaining evidence that can resolve questions of fraud before benefits are ever paid. SSA's plan to develop a national common disability case processing system will be a significant boost to its fraud detection capabilities.

There is also promise in private industry volunteered data. For example, the banking industry agreed to provide the federal government with information on payroll deposits to help track

illegitimate unemployment insurance claims. According to those in the banking/financial community, two areas that typically provide huge opportunities for fraud detection are: (1) detailed transactional financial histories and (2) data sources that identify individuals who have fallen off the grid, who may have relocated, died or gone underground to avoid payment of debts. As a cautionary note, government use of proprietary databases will likely require the establishment of a "Chinese data wall" to ensure that the government is not inappropriately in possession of proprietary data and that use of such data is consistent with federal privacy laws.

SSA should also explore potential partnerships with other government agencies that are coordinating efforts to combat fraud, waste, and abuse. The Department of Health and Human Services and the Department of Justice joined forces to develop the Health Care Fraud Prevention and Enforcement Action Team (HEAT) with a focus on cracking down on the people and organizations who abuse the Medicare and Medicaid system. HEAT's mission includes gathering resources across the government to help prevent waste, fraud, and abuse in the Medicare and Medicaid programs. The HEAT network could be a possible resource that SSA can leverage in expanding its data sources.

SSA must prioritize current efforts to improve its IT infrastructure to accommodate new fraud detection technologies and strengthen information security measures.

GAO recently determined that SSA had made strides in modernizing its IT systems to address growing workload demands, but also faced challenges associated with these modernization efforts and in correcting internal weaknesses in information security. In the course of the Academy's current work with SSA to develop a long-term strategic plan, SSA has conveyed an interest in improving its IT infrastructure. As part of this effort, SSA should determine how databases throughout the Administration, regional offices, field offices and State DDS offices can be integrated. When aggregated, the data maintained by these offices serves as a powerful tool for deriving patterns indicative of fraudulent activity. Furthermore, information silos make it easier for fraudsters to succeed. Data integration will enhance SSA's ability to manage and protect information it is responsible for safeguarding.

SSA should incorporate clear warnings to claimants and their representatives on the consequences of defrauding the disability insurance program early in the application process.

Making applicants aware of SSA's heightened efforts and capacity for combatting fraud provides another level of deterrence. In addition to implementing the newest available fraud detection technology, application documents should include warnings on the consequences of defrauding the federal disability insurance program. These efforts should also include an explanation of what activities are considered fraud, applicable statutes for prosecuting fraud, and the consequential civil and criminal penalties. This information must be provided at the earliest stage of the disability application and reinforced throughout the claims process.

SSA must send a clear message to claimants and their representatives on SSA's capacity to verify the validity of information provided throughout the claims process. This should include information on partnerships developed for the purposes of combatting fraud, waste, and abuse such as the CDI Program's ability to pool resources from State DDS offices and State and local law enforcement agencies. SSA's *my* Social Security portal would be an additional platform to ensure wide distribution of this information to applicants. Additional activities aimed at sending a strong warning to potential fraudsters can be incorporated across SSA regional and field offices and State DDS offices, for example, widespread publication of updates on CDI's successes in detecting and preventing fraud.

SSA must develop a culture of prevention and detection that extends to all employees.

Fraud typically occurs with a systemic or management error that is exploited by fraudsters. SSA must prioritize development of a work environment with a clear mission of fraud prevention and detection to enhance its capacity for identifying vulnerable business processes. As SSA has stated, they have relied on field office and DDS employees as a "first and best line of defense against fraud." In addition to front line employees, SSA must follow through on its plan to extend fraud detection training to all SSA employees. The content of this training must be regularly updated and revamped to optimize its capacity for engaging employees. Furthermore,

employees must be educated about data analysis tools and other technologies that contribute to SSA's mission to combat fraud.

Training efforts should include rewarding vigilance among employees through recognition and a performance appraisal system. Recognition will foster a culture of detecting and reporting fraud and may inspire innovation among employees to develop new ideas on fraud prevention.

Additional ethics training for supervisors and employees that is focused on a mission of protecting the American taxpayer and individuals who are truly disabled will also bolster a culture of fraud prevention. Ethical training may also serve as a tool for deterring employees from facilitating fraudulent activities such as those that were allegedly involved in the Puerto Rico conspiracy.

Consideration should also be given to creating a senior level executive position whose primary responsibility is to oversee and manage SSA's fraud detection and prevention efforts. This will enhance SSA's ability to identify and responds more readily to vulnerable business processes and systematize continuous improvements of fraud detection efforts. The responsibilities for this position should include collaboration with the private sector to ensure that SSA keeps pace with the best and latest technology available.

Conclusion

SSA is responsible for managing the largest disability insurance program in the world, providing $12 billion in monthly benefits to 11 million workers and their families. An operation of this magnitude will always be a target for fraud and abuse, but SSA is on the right path to a more robust approach to mitigating the scale of facilitator fraud. Investing in new analytic tools, integrating and expanding its data sources, increasing applicant awareness of SSA fraud prevention efforts and the consequences of defrauding the federal government, and fostering a culture of fraud prevention among all employees will assist SSA in achieving its stated goals of strengthening its anti-fraud activities and continuing to earn the public's trust in its stewardship of the disability program.